

\mathbf{F} field; f a polynomial in $\mathbf{F}[x]$, \mathbf{F}_f a splitting field of f over \mathbf{F} .

Examples:

(1) $f = x^2 - 2 \in \mathbf{Q}[x]$, $\mathbf{Q}_f = \mathbf{Q}(\sqrt{2})$:

f is irreducible in $\mathbf{Q}[x]$: if it were reducible, it could only decompose into the product of two linear factors $(x - \alpha)(x - \beta)$, with α, β zeroes of f : impossible over \mathbf{Q} , since the zeroes of f are $\pm\sqrt{2}$, which are irrational.

A splitting field of f over \mathbf{Q} is $\mathbf{Q}(\sqrt{2}, -\sqrt{2})$: over this field f splits into linear factors $f(x) = (x - \sqrt{2})(x + \sqrt{2})$.

It remains to observe that $\mathbf{Q}(\sqrt{2}, -\sqrt{2}) = \mathbf{Q}(\sqrt{2})$: a field which contains $\sqrt{2}$ necessarily contains also $-\sqrt{2}$.

(2) $f = x^2 - 2 \in \mathbf{R}[x]$, $\mathbf{R}_f = \mathbf{R}$:

f is reducible in $\mathbf{R}[x]$, since $\pm\sqrt{2} \in \mathbf{R}$. Hence $\mathbf{R}_f = \mathbf{R}$.

(3) $f = x^2 + 1 \in \mathbf{Q}[x]$, $\mathbf{Q}_f = \mathbf{Q}(i)$:

f is irreducible in $\mathbf{Q}[x]$: if it were reducible, it could only decompose into the product of two linear factors $(x - \alpha)(x - \beta)$, with α, β zeroes of f : impossible, since the zeroes of f are $\pm i$, which are complex numbers.

A splitting field of f over \mathbf{Q} is $\mathbf{Q}(i, -i) = \mathbf{Q}(i)$: over this field f splits into linear factors $f(x) = (x - i)(x + i)$.

(4) $f = x^2 + 1 \in \mathbf{R}[x]$, $\mathbf{R}_f = \mathbf{R}(i) = \mathbf{C}$:

From the above discussion it also follows that a splitting field of f over \mathbf{R} is $\mathbf{R}(i, -i) = \mathbf{R}(i) = \mathbf{C}$.

(5) $f = x^3 - 1 \in \mathbf{Q}[x]$, $\mathbf{Q}_f = \mathbf{Q}(\omega)$, where $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$:

f is reducible in $\mathbf{Q}[x]$, as $x^3 - 1 = (x - 1)(x^2 + x + 1)$, with $x^2 + x + 1$ irreducible in $\mathbf{Q}[x]$. The zeroes of $x^2 + x + 1$ are ω and $\bar{\omega} = \omega^2$.

A splitting field of f over \mathbf{Q} is $\mathbf{Q}(\omega, \omega^2) = \mathbf{Q}(\omega)$: over this field f splits into linear factors $f(x) = (x - 1)(x - \omega)(x - \omega^2)$.

(6) $f = x^3 - 1 \in \mathbf{R}[x]$, $\mathbf{R}_f = \mathbf{R}(\omega) = \mathbf{C}$:

From the discussion in (d) it also follows that a splitting field of f over \mathbf{R} is $\mathbf{R}(\omega, \omega^2) = \mathbf{R}(\omega)$

It remains to observe that $\mathbf{R}(\omega) = \mathbf{C}$: this follows from the fact that $i = \frac{1}{\sqrt{3}}(\omega - \omega^2) \in \mathbf{R}(\omega)$.

(7) $f = x^3 - 2 \in \mathbf{Q}[x]$, $\mathbf{Q}_f = \mathbf{Q}(\sqrt[3]{2}, \omega)$:

f is irreducible in $\mathbf{Q}[x]$: its roots in \mathbf{C} are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$.

A splitting field of f over \mathbf{Q} is $\mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$.

It remains to show that $\mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbf{Q}(\sqrt[3]{2}, \omega)$:

since $\omega = \sqrt[3]{2}\omega^2 / \sqrt[3]{2}\omega$ we have the inclusion $\mathbf{Q}(\sqrt[3]{2}, \omega) \subset \mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$. The other inclusion is obvious.

Excercise. Consider the real number $\alpha = \sqrt{2} + \sqrt[3]{2}$. Determine the minimal polynomial of α in $\mathbf{Q}[x]$.

Sol.: We look for a *monic* polynomial in $\mathbf{Q}[x]$, vanishing in α , and of minimum degree among the polynomials with these properties.

We construct the minimal polynomial of α in two stages:

- (a) we determine a monic polynomial f in $\mathbf{Q}[x]$ vanishing on α ;
- (b) we prove that the degree $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ equals the degree of f . From this we conclude that f is irreducible and therefore is the minimal polynomial of α in $\mathbf{Q}[x]$.

(a) Write $\sqrt[3]{2} = \alpha - \sqrt{2}$.

Raising both terms of the above equality to the 3^{rd} power we get

$$\begin{aligned} 2 &= (\alpha - \sqrt{2})^3 = \alpha^3 - 2\sqrt{2}\alpha^2 + 6\alpha - 2\sqrt{2} \\ &\Leftrightarrow \alpha^3 + 6\alpha - 2 = \sqrt{2}(3\alpha^2 + 2). \end{aligned} \tag{1}$$

After squaring both terms of the above equality, all roots have disappeared, and we see that α is a zero of the degree 6 polynomial in $\mathbf{Z}[x]$

$$f(x) = x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4.$$

We deduce that $[\mathbf{Q}(\alpha) : \mathbf{Q}] \leq 6$.

Recall that, since f is monic and $f(\alpha) = 0$,

f is the minimal polynomial of α

$$\Leftrightarrow f \text{ is irreducible in } \mathbf{Q}[x]$$

$$\Leftrightarrow [\mathbf{Q}(\alpha) : \mathbf{Q}] = \deg(f) = 6.$$

(b) Eisenstein's criterion for irreducibility does not apply to f : the prime $p = 2$ divides all coefficients, except the leading one, however $p^2 = 4$ does divide the constant term. Hence checking the irreducibility of f directly may require quite a bit of work...

Instead we choose to prove that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 6 = \deg(f)$, using field theory.

If we show that both $\mathbf{Q}(\sqrt{2})$, which an extension of \mathbf{Q} of degree 2, and $\mathbf{Q}(\sqrt[3]{2})$, which an extension of \mathbf{Q} of degree 3, are subfields of $\mathbf{Q}(\alpha)$, then the multiplicativity of degrees implies that 2 and 3 divide $[\mathbf{Q}(\alpha) : \mathbf{Q}]$. It follows that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 6$ and that f is the desired minimal polynomial of α .

In order to do that it is sufficient to observe that $\sqrt{2}$ and $\sqrt[3]{2}$ lie in $\mathbf{Q}(\alpha)$: from (1) we have that $\sqrt{2} = \frac{\alpha^3 + 6\alpha - 2}{3\alpha^2 + 2}$, a rational function of α , lies in $\mathbf{Q}(\alpha)$; then also $\sqrt[3]{2} = \alpha - \sqrt{2}$ lies in $\mathbf{Q}(\alpha)$. This finishes the proof of (b).

Conclusion: the minimal polynomial of α is $f(x) = x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$.